REMARKS

In the Final Office Action mailed February 21, 2006, the Examiner considered claims 1-30. Claims 1-30 stand rejected. For the reasons set forth below, Applicant respectfully requests the Examiner reconsider the rejections and allow all the pending claims.

Examiner Interview Summary

A telephone interview was held on May 2, 2006 between Examiner Aravind Moorthy and the attorney for the Applicant, Thomas George, to discuss the Final Office Action mailed February 21, 2006. With respect to the Section 112 rejection, Mr. George explained that the Applicant's specification does not state that a particular element is an essential element and thus no element is required to be in a claim. Mr. George pointed out that support for claims 19 and 20 is found in Applicant's specification at, e.g., pg. 20, lns. 14-22. The Examiner indicated that he would reconsider the Section 112 rejection.

With respect to the Section 102 rejection, for claims 1, 4, 8, 13, 15, and 16, Mr. George explained that *Grawrock*, as shown by FIG. 2, discloses that only the password is hashed rather than "performing a hashing algorithm on the hint and the password" as set forth in these claims. For claims 1, 4, 8, 13, 15, and 16, Mr. George explained that *Grawrock* discloses sending an "encrypted key" to an "authenticating entity 299" (as shown by *Grawrock* at col. 4, lns. 11-13; and col. 5, ln. 43 to col. 6, ln. 27) rather than "sending the encrypted data" to a server or client as set forth in these claims. Mr. George also pointed out that *Grawrock* discloses a computer security system that includes a "computer system 200" and an "authenticating entity 299", but this is not a client-server system.

Mr. George explained that *Challener* discloses generating a password by concatenating and then hashing a "relatively secret key" and the computer's serial number. For claims 3, 7, and 22, Mr. George explained that *Challener* discloses generating a password, but does not disclose hashing the password as set forth in those claims. For claims 3 and 7, Mr. George explained that *Challener* discloses performing the hashing operation only once (i.e., hashing the concatenation of the "relatively secret key" and the computer's serial number) rather than performing the hashing operation multiple times as set forth in those claims. In addition, Mr. George explained that

Challener does not disclose a client-server system.

The Examiner indicated that he would reconsider the Section 102 rejections and possibly perform another prior art search.

Rejections Under 35 U.S.C. § 112

Claims 19 and 20 have been rejected under 35 U.S.C. § 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. MPEP § 2172.01.

MPEP § 2172.01 states that matter described to be essential in the specification should not be omitted from the claims. However, nowhere in Applicant's specification is it stated that "deriving the key" requires some essential element, and thus a particular element is not required to be in the claim. Claim 19 recites, *inter alia*: (i) a "decryption downloadable", sent to a client, that derives "a key from a password and a hint", and (ii) "deriving the key by hashing at least one of the hint and the password." Support for claim 19 is found in Applicant's specification at, e.g., pg. 20, lns. 14-22. Neither this portion nor any other part of the specification specify that an essential element is required and thus claim 19 is not required to recite a particular element.

Similarly, with respect to claim 20, nowhere in Applicant's specification is it stated that "deriving a key" requires some essential element, and thus a particular element is not required to be in the claim. Support for claim 20 is found in Applicant's specification at, e.g., pg. 20, lns. 14-22.

For the foregoing reasons, the Applicant submits that claims 19 and 20 satisfy the requirements of 35 U.S.C. 112, second paragraph, and withdrawal of the rejection is respectfully requested.

Rejections Under 35 U.S.C. § 102(e)

(a) Claims 1-2, 4-6, and 8-19

Claims 1-2, 4-6, and 8-19 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 6,360,322 to Grawrock ("*Grawrock*").

With respect to independent claims 1 and 8, the Applicant submits that *Grawrock* does not disclose the elements set forth in claims 1 and 8, which include, *inter alia*, (i) "performing a hashing

algorithm on the hint and the password to generate a key", (ii) "encrypting data using the key", and (iii) "sending the encrypted data to a server for storage". For (i), the Examiner asserts that col. 6, ln. 52 to col. 7, line 27 of *Grawrock* discloses this element. However, this portion of *Grawrock* discloses that only the password is hashed rather than "performing a hashing algorithm on the hint and the password" as recited in claims 1 and 8; for example, col. 6, lns. 54-55 of *Grawrock* states that the "hash of the entered user password is taken" but there is no mention in *Grawrock* that another item (e.g., "question") is also hashed. In fact, as shown in FIG. 2 of *Grawrock*, the "hash function 262" has only the "user password" as its input. Thus, *Grawrock* does not disclose "performing a hashing algorithm on the hint and the password" as recited in claims 1 and 8. For (ii), the Examiner asserts that col. 6, ln. 52 to col. 7, ln. 27 of *Grawrock* discloses this element. However, this portion of *Grawrock* discloses that "all $File_i$ are encrypted with a K_{fi}", but "K_{fi}" is not a "key" generated by "performing a hashing algorithm on the hint and the password" as set forth in claims 1 and 8. Thus, *Grawrock* does not disclose "encrypting data using the key" as recited in claims 1 and 8 where the key is generated by "performing a hashing algorithm on the hint and the password." For (iii), the Examiner asserts that col. 6, ln. 52 to col. 7, ln. 27 of *Grawrock* discloses this element. However, *Grawrock* discloses sending an encrypted "K_{acc2}" to "authenticating entity 299"; however, "K_{acc2}" is an "access key" rather than data. (*Grawrock* at col. 4, lns. 11-13; and col. 5, ln. 43 to col. 6, ln. 27). In addition, *Grawrock* discloses that the "authenticating entity 299" sends back to the "computer system 200" the "K_{acc2}" which, as stated earlier, is an "access key" rather than data. (*Grawrock* at col. 7, lns. 10-12). Thus, *Grawrock* does not disclose "sending the encrypted data to a server for storage" as set forth in claims 1 and 8.

For at least the foregoing reasons, the Applicant respectfully requests reconsideration and allowance of claims 1 and 8. Claim 2 depends from claim 1, and claims 9-10 depend from claim 8. Accordingly, these dependent claims are also patentable over *Grawrock* for at least the reasons provided earlier with respect to claims 1 and 8.

With respect to independent claim 4, the Applicant submits that *Grawrock* does not disclose the elements set forth in claim 4, which include, *inter alia*, (i) "a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key", (ii) "an encryption engine coupled to the key generator for encrypting data using the key", and (iii) "a communications module coupled to the engine for sending the encrypted data and the

hint to a server for storage". For reasons similar to those provided earlier with respect to claims 1 and 8, the Applicant asserts that claim 4 is also patentable over *Grawrock*. Claims 5-6 depend from claim 4 and so the Applicant asserts that these two claims are also patentable over *Grawrock*.

With respect to independent claim 11, the Applicant submits that *Grawrock* does not disclose the elements set forth in claim 11, which include, *inter alia*, (i) "receiving a request to store encrypted data from a client", (ii) "sending an encryption downloadable for deriving a key to encrypt data to the client", and (iii) "receiving encrypted data that was encrypted by the encryption downloadable from the client". For (i), the Examiner asserts that col. 2, lns. 54-62 of *Grawrock* discloses this element. However, this portion of *Grawrock* discloses encrypting "file data", but there is no mention of "receiving a request . . . from a client" as set forth in claim 11. For (ii), the Examiner asserts that col. 3, lns. 5-13 of *Grawrock* disclose this element. However, this portion of *Grawrock* discloses a "file encryption key K_{fi}" rather than an "encryption downloadable for deriving a key" as set forth in claim 11. Also, this portion of *Grawrock* does not disclose "sending an encryption downloadable . . . to the client" as set forth in claim 11; in fact, it does not disclose sending anything to a client since *Grawrock* does not disclose a client-server system. For (iii), the Examiner asserts that col. 3, lns. 14-22 of *Grawrock* discloses this element. However, this portion of *Grawrock* discloses encrypting the access key "K_{fi}"; however, this portion nor anywhere else in *Grawrock* discloses "receiving encrypted data . . . from the client" as set forth in claim 11. For at least the foregoing reasons, the Applicant respectfully requests reconsideration and allowance of claim 11.

With respect to independent claim 12, the Applicant submits that *Grawrock* does not disclose the elements set forth in claim 12, which include, *inter alia*, "a web server for interfacing with a client, for sending the encryption downloadable to the client, and for receiving encrypted data that was encrypted by the encryption downloadable from the client." The Examiner asserts that col. 3, lns. 5-13 of *Grawrock* discloses this element. This portion of *Grawrock* discloses encrypting the "encryption key K_{fi}" using the "encrypting unit 218"; however, this portion does not disclose a "web server", nor receiving "encrypted data . . from the client" as set forth in claim 12. For at least these reasons, the Applicant respectfully requests reconsideration and allowance of claim 12.

With respect to independent claims 13, 15, and 16, the Applicant submits that *Grawrock* does not disclose the elements set forth in these claims, which include, *inter alia*, "sending encrypted data and a hint corresponding to the encrypted data from a server to a client" and "performing a hashing algorithm on the password and the hint at the client to generate a key for decrypting the encrypted data". The Examiner asserts that col. 5, lns. 1-42 of *Grawrock* discloses the "sending" element. This portion of *Grawrock* discloses sending an "OT private key" and "various identifying information" to the "authenticating entity"; however, the cited portion does not disclose "sending encrypted data . . . to a client" as set forth in claims 13, 15, and 16. With respect to the "performing" element, for the reasons provided earlier with respect to claims 1 and 8, the Applicant asserts that *Grawrock* does not disclose this element. For at least these reasons, the Applicant respectfully requests reconsideration and allowance of claims 13, 15, and 16. Claim 14 depends from claim 13, and claims 17-18 depend from claim 16. Thus, for the reasons provided earlier with respect to the independent claims, these dependent claims are also patentable over *Grawrock.*

With respect to independent claim 19, the Applicant submits that *Grawrock* does not disclose the elements set forth in claim 19, which include, *inter alia*, "sending a decryption downloadable for deriving a key from a password and a hint to a client". The Examiner asserts that col. 5, lns. 1-42 of *Grawrock* discloses this element. This portion of *Grawrock* discloses sending an "OT private key" and "various identifying information" to the "authenticating entity 299"; however, the cited portion does not disclose that the "authenticating entity 299" uses a "password" and no "password" is ever sent to the "authenticating entity 299", and thus the "authenticating entity 299" is not sent "a decryption downloadable for deriving a key from a password and a hint" as set forth in claim 19. For at least this reason, the Applicant respectfully requests reconsideration and allowance of claim 19.

(b) Claims 3, 7, and 20-30

Claims 3, 7, and 20-30 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent No. 6,470,454 to Challener ("*Challener*").

With respect to independent claim 3, the Applicant submits that *Challener* does not disclose the elements set forth in claim 3, which include, *inter alia*, (i) "performing a hashing

algorithm on the hint and the password to generate a key, wherein the step of performing a hashing algorithm includes hashing the password to derive a first secret, hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key", (ii) "encrypting data using the key", and (iii) "sending the encrypted data to a server for storage". For (i), the Examiner asserts that col. 5, ln. 51 to col. 6, ln. 33 of *Challener* discloses this element. This portion of *Challener* discloses generating a "computer system configuration password" by obtaining the computer's serial number and a "relatively secret key" known only to the support organization, and these two items are concatenated together and then hashed to generate the password. *Challener* does not disclose, *inter alia*, "hashing the password to derive a first secret" as set forth in claim 3 because *Challener* discloses that the hashing function is performed to generate the password but the password is not one of the items that is hashed. In addition, *Challener* discloses that the "relatively secret key" is obtained from the support organization, rather than "derive a first secret" by hashing the password as set forth in claim 3. Also, *Challener* discloses performing only a single hashing function on the concatenation of the password and the "relatively secret key", but does not disclose performing multiple hash functions such as, e.g., "hashing the first secret to derive a second secret", "hashing the hint and the first secret to generate an intermediate index", and "hashing the intermediate index and the second secret" as set forth in claim 3. In addition, *Challener* discloses that the hashing function generates a "password", rather than generate the "key", the "intermediate index", the "second secret", or the "first secret" as set forth in claim 3. For (ii), *Challener* does not disclose "encrypting data" and in fact, the word "encrypt" is not mentioned anywhere in *Challener*. For (iii), *Challener* discloses obtaining the "computer's serial number" (this is not encrypted) from the computer user, rather than "sending the encrypted data to a server for storage" as set forth in claim 3. For at least the foregoing reasons, the Applicant respectfully requests reconsideration and allowance of claim 3.

With respect to independent claim 7, for similar reasons provided with respect to claim 3, the Applicant submits that *Challener* does not disclose the elements set forth in claim 7, which include, *inter alia*, (i) "a key generator coupled to the user interface for performing a hashing algorithm on a hint and the password to generate a key wherein the key generator hashes the

password to derive a first secret, hashes the first secret to derive a second secret, hashes the hint and the first secret to generate an intermediate index, and hashes the intermediate index and the second secret to generate the key", (ii) "an encryption engine coupled to the key generator for encrypting data using the key", and (iii) "a communications module coupled to the engine for sending the encrypted data to a server for storage".

With respect to independent claim 20, the Applicant submits that *Challener* does not disclose the elements set forth in claim 20, which include, *inter alia*, (i) "a decryption downloadable for deriving a key by hashing at least one of a password and a hint", (ii) "encrypted data", and (iii) "a web server for interfacing with a client, and for sending the decryption downloadable, the encrypted data and the hint to the client". For (i), *Challener* discloses deriving a "password", rather than "a decryption downloadable for deriving a key by hashing at least one of a password and a hint" as set forth in claim 20. For (ii), *Challener* does not disclose "encrypted data" and in fact, the word "encrypt" is not mentioned anywhere in *Challener*. For (iii), *Challener* discloses that the "consultant" performs the hashing function at his computer and the only item received/sent from another entity is the "computer's serial number" (this number is not encrypted) which is obtained from the computer user. However, the computer user is not a client and thus at least for this reason, *Challener* does not disclose "a web server for interfacing with a client, and for sending the decryption downloadable, the encrypted data and the hint to the client". For at least the foregoing reasons, the Applicant respectfully requests reconsideration and allowance of claim 20.

With respect to independent claims 21 and 26, the Applicant submits that *Challener* does not disclose the elements set forth in claims 21 and 26, which include, *inter alia*, (i) "deriving a first secret from the password", (ii) "deriving an intermediate index from the first secret and the hint", and (iii) "sending the intermediate index to the server". For (i), the Examiner asserts that col. 5, lns. 28-50 of *Challener* discloses this element. This portion of *Challener* discloses generating a password using the computer's serial number and a "relatively secret key", which is almost the opposite of "deriving a first secret from the password" as set forth in claims 21 and 26. For (ii), the Examiner asserts that col. 5, ln. 59 to col. 6, ln. 33 of *Challener* discloses this element. This portion of *Challener* discloses generating a password using the computer's serial number and a "relatively secret key", rather than "deriving an intermediate index from the first

secret and the hint" as set forth in claims 21 and 26. For (iii), the Examiner asserts that col. 5, ln. 59 to col. 6, ln. 33 of *Challener* discloses this element. This portion of *Challener* discloses receiving the computer's serial number from the computer user, rather than "sending the intermediate index to the server" as set forth in claims 21 and 26.

For the foregoing reasons, the Applicant asserts that claims 21 and 26 are patentable over *Challener*. Claims 22-23 depend from claim 21, and claims 27-28 depend from claim 26. Thus, the Applicant asserts that these dependent claims are also patentable over *Challener*.

With respect to independent claim 24, the Applicant submits that *Challener* does not disclose the elements set forth in claim 24, which include, *inter alia*, (i) "an index generator coupled to the user interface for generating an intermediate index from a hint received from a server and a secret derived from the password", and (ii) "a communications engine coupled to the index generator for sending the intermediate index to the server." For (i), the Examiner asserts that col. 5, ln. 59 to col. 6, ln. 33 of *Challener* discloses this element. This portion of *Challener* discloses generating a password using the computer's serial number and a "relatively secret key", rather than an "index generator" that generates an intermediate index using in part "a secret derived from the password" as set forth in claim 24. For (ii), the Examiner asserts that col. 5, ln. 59 to col. 6, ln. 33 of *Challener* discloses this element. This portion of *Challener* discloses receiving the computer's serial number from the computer user, rather than "a communications engine coupled to the index generator for sending the intermediate index to the server" as set forth in claim 24. For the foregoing reasons, the Applicant asserts that claim 24 is patentable over *Challener*. Claim 25 depends from claim 24, and thus, the Applicant asserts that it is also patentable over *Challener*.

With respect to independent claims 29, the Applicant submits that *Challener* does not disclose the elements set forth in claims 29, which include, *inter alia*, (i) "receiving an indication of encrypted data to be decrypted", (ii) "transmitting to a client a hint corresponding to the indication, and a decryption downloadable for deriving an intermediate index from a password and the hint", (iii) "receiving the intermediate index from the client", and (iv) "deriving a decryption key from a second secret corresponding to the user and the intermediate index." For (i), the Examiner asserts that col. 6, lns. 21-57 of *Challener* discloses this element. However, there is no indication in *Challener* that any data is ever encrypted. For (ii), the Examiner asserts

that col. 6, lns. 21-57 of *Challener* discloses this element. This portion of *Challener* discloses deriving a password rather than "deriving an intermediate index from a password and the hint" as set forth in claim 29. For (iii), the Examiner asserts that col. 5, ln. 59 to col. 6, ln. 33 discloses this element. This portion of *Challener* discloses receiving the computer's serial number from the computer user, rather than "receiving the intermediate index from the client" as set forth in claim 29. For (iv), the Examiner asserts that col. 5, ln. 59 to col. 6, ln. 33 of *Challener* discloses this element. This portion discloses generating a password using the computer's serial number and a "relatively secret key", however, it does not disclose "deriving a decryption key" or the "second secret" set forth in claim 29. For the foregoing reasons, the Applicant asserts that claim 29 is patentable over *Challener*.

With respect to independent claim 30, the Applicant submits that *Challener* does not disclose the elements set forth in claim 30, which include, *inter alia*, (i) "a decryption downloadable for generating an intermediate index from a password and a hint", (ii) "a web server for receiving an indication of encrypted data to be decrypted, for transmitting the decryption downloadable and a hint corresponding to the indication to a client, and for receiving an intermediate index from the client", and (iii) "a server-resident module for deriving a key for decrypting the encrypted data from the second secret and the intermediate index." For (i), the Examiner asserts that col. 6, lns. 21-57 of *Challener* discloses this element. This portion of *Challener* discloses generating a password using the computer's serial number and a "relatively secret key", rather than "a decryption downloadable for generating an intermediate index from a password and a hint" as set forth in claim 30. For (ii), the Examiner asserts that col. 5, ln. 59 to col. 6, ln. 33 of *Challener* discloses this element. This portion of *Challener* discloses receiving the computer's serial number from the computer user in order to generate the password, but *Challener* does not disclose generating an intermediate index. The "computer user" of *Challener* is not a "web server" set forth in claim 30, nor does *Challener* disclose, *inter alia*, the "intermediate index" set forth in claim 30. For (iii), the Examiner asserts that col. 5, ln. 59 to col. 6, ln. 33 of *Challener* discloses this element. This portion of *Challener* discloses generating a "password"; however, it does not disclose a "server-resident module for deriving a key", "encrypted data", "second secret", and "intermediate index" as set forth in claim 30.

CONCLUSION

On the basis of the above remarks, reconsideration and allowance of all the pending claims is believed to be warranted and such action is respectfully requested. If the Examiner has any questions or comments, the Examiner is respectfully requested to contact the undersigned at the number listed below. The Office is hereby authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1847.

Respectfully submitted,

Thomas George
Registration No. 45,740
MANATT, PHELPS & PHILLIPS LLP
1001 Page Mill Road, Building 2
Palo Alto, California 94304
650-812-1327 Telephone
650-213-0286 Facsimile

20155978.1